REMARKS

1. Applicant thanks the Examiner for the Examiner's comments which have greatly assisted Applicant in responding.

Applicant has amended Claims 1, 5, 6, 10, 14, 15, 19, 23, and 24. It should be noted that Applicant has elected to amend said Claims solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent Business Goals, 65 Fed. Reg. 54603 (9/8/00). In making this amendment, Applicant has not and does not in any way narrow the scope of protection to which Applicant considers the invention herein to be entitled and does not concede, in any way, that the subject matter of such Claims was in fact taught or disclosed by the cited prior art. Rather, Applicant reserves Applicant's right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

2. 35 U.S.C. §103(a). The Examiner has rejected Claims 1-4, 6-13, 15-22, and 24-27 under 35 U.S.C. §103(a) as being unpatentable over Liles et al. (U.S. Patent No. 5,880,731), Albrecht et al. (U.S. Patent No. 5,950,011), Janis (U.S. Patent No. 5,263,165), and Cutler et al. (U.S. Patent No. 5,129,083).

Applicant respectfully disagrees.

Claims 1, 10, and 19:

Claims 1, 10 , and 19 have been amended to clarify the invention and appear as follows:

1. A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined access control command attribute read list containing user identifications that are allowed to read a specified set of Lightweight Directory Access Protocol (LDAP) attributes;

providing a system administrator defined read access control command;

wherein said read access control command resides in a directory containing said LDAP attributes;

said read access control command listing LDAP user attributes that said administrator has selected for user defined read access; and

said read access control command referring to said user defined read list at runtime thereby allowing said read user identifications read access to said LDAP user attributes.

10. An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a user defined access control command attribute read list containing user identifications that are allowed to read a specified set of Lightweight Directory Access Protocol (LDAP) attributes; and

a system administrator defined read access control command;

wherein said read access control command resides in a directory containing said LDAP attributes;

wherein said read access control command lists LDAP user attributes that said administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list at runtime thereby allowing said read user identifications read access to said LDAP user attributes.

19. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined access control command attribute read list containing user identifications that are allowed to read a specified set of Lightweight Directory Access Protocol (LDAP) attributes;

providing a system administrator defined read access control command;

wherein said read access control command resides in a directory containing said LDAP attributes;

said read access control command listing LDAP user attributes that said administrator has selected for user defined read access; and

said read access control command referring to said user defined read list at runtime thereby allowing said read user identifications read access to said LDAP user attributes.

In particular, neither Liles, Albrecht, Janis, nor Cutler, teach, describe, or contemplate a system that provides a user defined access control command attribute read list containing user identifications that are allowed to read a specified set of Lightweight Directory Access Protocol (LDAP) attributes as claimed in the invention. Nor do the cited references teach, describe, or contemplate a system that provides a system administrator defined read access control command, wherein the read access control command resides in a directory containing the LDAP attributes as claimed in the invention. Neither Liles, Albrecht, Janis, nor Cutler attempt to address the problems associated with millions of LDAP entries on an LDAP server with millions of access control commands and therefore do not contemplate the invention as claimed.

A unique feature of the invention is that the system administrator has complete control over what a user can do with respect to the user's LDAP attributes. Also, the ability of the user to define read and write list access control command attributes which are plugged into the system administrator defined read and write access control commands at runtime, dramatically reduces the number of access control commands in the LDAP directory required to manage the server's LDAP directories. Having the user restricted to defining read and write lists simplifies the user's task by not requiring the user to understand access control command syntax.

To combine Liles, Albrecht, Janis, and Cutler based on singular terms such as "user defined", "access control command", and "read access" as the Office Action suggests requires information gleaned from the present invention. Such use of hindsight is impermissible.

Therefore, Liles, Albrecht, Janis, and Cutler do not teach or disclose the invention as claimed.

Claims 1, 10, and 19 are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 6, 15, and 24:

Claims 6, 15, and 24 have been amended to clarify the invention and appear as follows:

6. A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined access control command attribute write list containing user identifications that are allowed to write a specified set of Lightweight Directory Access Protocol (LDAP) attributes;

providing a system administrator defined write access control command;

wherein said write access control command resides in a directory containing said LDAP attributes;

said write access control command listing LDAP user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list at runtime thereby allowing said write user identifications write access to said LDAP user attributes.

15. An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a user defined access control command attribute write list containing user identifications that are allowed to write a specified set of Lightweight Directory Access Protocol (LDAP) attributes; and

a system administrator defined write access control command;

wherein said write access control command resides in a directory containing said LDAP attributes;

wherein said write access control command lists LDAP user attributes that said administrator has selected for user defined write access; and

wherein said write access control command refers to said user defined write list at runtime thereby allowing said write user identifications write access to said LDAP user attributes.

24. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined access control command attribute write list containing user identifications that are allowed to write a specified set of Lightweight Directory Access Protocol (LDAP) attributes;

providing a system administrator defined write access control command;

wherein said write access control command resides in a directory containing said LDAP attributes;

said write access control command listing LDAP user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list at runtime thereby allowing said write user identifications write access to said LDAP user attributes.

As with Claims 1, 10, and 19, above, neither Liles, Albrecht, Janis, nor Cutler, teach, describe, or contemplate a system that provides a user defined access control command attribute write list containing user identifications that are allowed to write a specified set of Lightweight Directory Access Protocol (LDAP) attributes, provides a

system administrator defined write access control command, and wherein the write access control command resides in a directory containing the LDAP attributes as claimed in the invention. Neither Liles, Albrecht, Janis, nor Cutler attempt to address the problems associated with millions of LDAP entries on an LDAP server with millions of access control commands and therefore do not contemplate the invention as claimed.

Therefore, Liles, Albrecht, Janis, and Cutler do not teach or disclose the invention as claimed.

Claims 6, 15, and 24 are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 2, 11, and 20:

The rejection of Claims 2, 11, and 20 is deemed moot in view of Applicant's remarks regarding Claims 1, 10, and 19, above. Claims 2, 11, and 20 are dependent upon independent Claims 1, 10, and 19, respectively, which are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 3, 12, and 21:

The rejection of Claims 3, 12, and 21 is deemed moot in view of Applicant's remarks regarding Claims 1, 10, and 19, above. Claims 3, 12, and 21 are dependent upon independent Claims 1, 10, and 19, respectively, which are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 4, 13, and 22:

The rejection of Claims 4, 13, and 22 is deemed moot in view of Applicant's remarks regarding Claims 1, 10, and 19, above. Claims 4, 13, and 22 are dependent upon independent Claims 1, 10, and 19, respectively, which are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 7, 16, and 25:

The rejection of Claims 7, 16, and 25 is deemed moot in view of Applicant's remarks regarding Claims 6, 15, and 24, above. Claims 7, 16, and 25 are dependent upon independent Claims 6, 15, and 24, respectively, which are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 8, 17, and 26:

The rejection of Claims 8, 17, and 26 is deemed moot in view of Applicant's remarks regarding Claims 6, 15, and 24, above. Claims 8, 17, and 26 are dependent upon independent Claims 6, 15, and 24, respectively, which are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 9, 18, and 27:

The rejection of Claims 9, 18, and 27 is deemed moot in view of Applicant's remarks regarding Claims 6, 15, and 24, above. Claims 9, 18, and 27 are dependent upon independent Claims 6, 15, and 24, respectively, which are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

3. 35 U.S.C. §103(a). The Examiner has rejected Claims 5, 14, and 23 under 35 U.S.C. §103(a) as being unpatentable over Janis, Albrecht, Liles, and Cutler.

Applicant respectfully disagrees.

Claims 5, 14, and 23 have been amended to clarify the invention and appear as follows:

5. A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined read access control command that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access;

providing a system administrator defined write access control command that lists LDAP user attributes that said administrator has selected for user defined write access;

providing a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said LDAP user attributes that said administrator has selected for user defined read access; and

providing a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP user attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute

being accessed are used to determine if said client has permission to execute said write access.

14. An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a system administrator defined read access control command that lists [the] Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access;

a system administrator defined write access control command that lists LDAP user attributes that said administrator has selected for user defined write access;

a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said LDAP user attributes that said administrator has selected for user defined read access; and

a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

23. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps

for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined read access control command that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access;

providing a system administrator defined write access control command that lists LDAP user attributes that said administrator has selected for user defined write access;

providing a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said LDAP user attributes that said administrator has selected for user defined read access;

providing a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

As with Claims 1, 10, and 19, above, neither Janis, Albrecht, Liles, nor Cutler, teach, describe, or contemplate a system that provides a system administrator defined read access control command that lists Lightweight Directory Access Protocol (LDAP) user attributes that the administrator has selected for user defined read access, provides a

system administrator defined write access control command that lists LDAP user attributes that the administrator has selected for user defined write access, and wherein the read access control command and the write access control command reside in a directory containing the LDAP attributes as claimed in the invention. Further, neither Janis, Albrecht, Liles, nor Cutler, teach, describe, or contemplate a system that provides a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read the LDAP user attributes that said administrator has selected for user defined read access, provides a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write the LDAP user attributes that said administrator has selected for user defined write access as claimed in the invention.

As stated above, neither Liles, Albrecht, Janis, nor Cutler attempt to address the problems associated with millions of LDAP entries on an LDAP server with millions of access control commands and therefore do not contemplate the invention as claimed.

To combine Janis, Albrecht, Liles, and Cutler based on singular terms such as "administrator has selected", "access control command", "read list", "for user defined", and "read access" as the Office Action suggests requires information gleaned from the present invention. Such use of hindsight is impermissible.

Therefore, Liles, Albrecht, Janis, and Cutler do not teach or disclose the invention as claimed.

Claims 5, 14, and 23 are in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

CONCLUSION

Based on the foregoing, Applicant considers the present invention to be distinguished from the art of record. Accordingly, Applicant earnestly solicits the Examiner's withdrawal of the rejections raised in the above referenced Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent.

Respectfully Submitted,

Michael A. Glenn
Reg. No. 30,176

Customer No. 22862

Version with markings to show changes made

In The Claims

Please amend Claim 1, 5, 6, 10, 14, 15, 19, 23, and 24 as follows (Marked copy):

1. (amended) A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined access control command attribute read list containing user identifications that are allowed to read a specified set of Lightweight Directory Access Protocol (LDAP) attributes;

providing a system administrator defined read access control command;

wherein said read access control command resides in a directory containing said LDAP attributes;

said read access control command listing [the] LDAP user attributes that said administrator has selected for user defined read access; and

said read access control command referring to said user defined read list at runtime thereby allowing said read user identifications read access to said LDAP user attributes.

5. (amended) A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined read access control command that lists [the] Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access;

providing a system administrator defined write access control command that lists [the] LDAP user attributes that said administrator has selected for user defined write access;

providing a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said LDAP user attributes that said administrator has selected for user defined read access; and

providing a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP user attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

6. (amended) A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined access control command attribute write list containing user identifications that are allowed to write a specified set of Lightweight Directory Access Protocol (LDAP) attributes;

providing a system administrator defined write access control command;

wherein said write access control command resides in a directory containing said LDAP attributes;

said write access control command listing [the] LDAP user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list at runtime thereby allowing said write user identifications write access to said LDAP user attributes.

10. (amended) An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a user defined access control command attribute read list containing user identifications that are allowed to read a specified set of Lightweight Directory Access Protocol (LDAP) attributes; and

a system administrator defined read access control command;

wherein said read access control command resides in a directory containing said LDAP attributes;

wherein said read access control command lists [the] LDAP user attributes that said administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list at runtime thereby allowing said read user identifications read access to said LDAP user attributes.

14. (amended) An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a system administrator defined read access control command that lists [the] Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access;

a system administrator defined write access control command that lists [the] LDAP user attributes that said administrator has selected for user defined write access;

a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said LDAP user attributes that said administrator has selected for user defined read access; and

a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

15. (amended) An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a user defined access control command attribute write list containing user identifications that are allowed to write a specified set of Lightweight Directory Access Protocol (LDAP) attributes; and

a system administrator defined write access control command;

wherein said write access control command resides in a directory containing said LDAP attributes;

wherein said write access control command lists [the] LDAP user attributes that said administrator has selected for user defined write access; and

wherein said write access control command refers to said user defined write list at runtime thereby allowing said write user identifications write access to said LDAP user attributes.

19. (amended) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined access control command attribute read list containing user identifications that are allowed to read a specified set of Lightweight Directory Access Protocol (LDAP) attributes;

providing a system administrator defined read access control command;

wherein said read access control command resides in a directory containing said LDAP attributes;

said read access control command listing [the] LDAP user attributes that said administrator has selected for user defined read access; and

said read access control command referring to said user defined read list at runtime thereby allowing said read user identifications read access to said LDAP user attributes.

23. (amended) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined read access control command that lists [the] Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access;

providing a system administrator defined write access control command that lists [the] LDAP user attributes that said administrator has selected for user defined write access;

providing a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said LDAP user attributes that said administrator has selected for user defined read access;

providing a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

24. (amended) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a user defined access control command attribute write list containing user identifications that are allowed to write a specified set of Lightweight Directory Access Protocol (LDAP) attributes;

providing a system administrator defined write access control command;

wherein said write access control command resides in a directory containing said LDAP attributes;

said write access control command listing [the] LDAP user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list at runtime thereby allowing said write user identifications write access to said LDAP user attributes.